

Amendments to the CLAIMS

1           1 – 18. (canceled)

1           19. (currently amended)     A system for device authentication, the system comprising:  
2                   a coprocessor security device configured to store a service provider data item and  
3           one or more device secretes ~~a device secret~~; and  
4                   a printer cartridge comprising a roaming security device, the roaming security  
5           device having the one or more devices secrets and a means for optionally generating a random  
6           number;  
7                   a host device configured to store a service provider data item and the one or more  
8           device secrets connected to the coprocessor security device, the host device configured to  
9           communicate with the coprocessor security device and a the printer cartridge, comprising the  
10          roaming security device, when the printer cartridge is removably installed in the host device  
11          ~~roaming security device~~, the roaming security device being configured to store a plurality of  
12          different service provider data items such that said roaming security device may communicate  
13          with a plurality of different service providers;  
14                  wherein the roaming security device can be authenticated to thereby enable  
15          operation of the host device.

1           20. – 22. (canceled)

1           23. (currently amended)     The system of claim 19 ~~20~~, wherein the printer cartridge is  
2          disabled responsive to the roaming security device being removed from the printer cartridge.

1           24. (currently amended)     A method of device authentication, the method comprising  
2     ~~the steps of:~~  
3                 receiving, at a printer cartridge comprising a roaming device, a challenge from a  
4     host printer device;  
5                 generating, at the printer cartridge comprising the roaming device, a first  
6     nonreversible computation result, wherein the first nonreversible computation result is computed  
7     by seeding a first nonreversible algorithm with at least the challenge, ~~a selected service provider~~  
8     ~~data item~~, and a roaming device secret;  
9                 outputting to the host printer device a response to the challenge, wherein the  
10    outputted response includes the first nonreversible computation result,  
11                 outputting to the host an identification and at least another data item ~~including~~  
12    ~~one of a plurality of service provider data items~~;  
13                 generating, at the host printer device a second nonreversible computation result,  
14    wherein the second nonreversible computation result is computed by seeding a second  
15    nonreversible algorithm with at least a challenge, ~~said selected service provider data item~~ and a  
16    host printer device secret;  
17                 comparing, by said host printer device, said first nonreversible computation and  
18    said second nonreversible computation in order to authenticate the printer cartridge comprising  
19    the roaming device;  
20                 allowing said host printer device to print documents if said printer cartridge  
21    comprising said roaming device is authenticated.

1           25. - 26. (canceled)

1           27. (currently amended)     The method of claim 24, further comprising:  
2                   enabling said printer cartridge to operate ~~an electronic device~~ responsive to a  
3     positive authentication of the roaming device.

1           28. (currently amended)     The method of claim 24, further comprising:  
2                   disabling said host printer device ~~an electronic device~~ responsive to a failure to  
3     authenticate the roaming device.

1           29. (previously submitted)   The method of claim 24, wherein the first nonreversible  
2     computation result is computed by further seeding the first nonreversible algorithm with a  
3     unique device identifier.

1           30. - 34. (canceled)

1           35.     (new) A host system device and subsystem device combination comprising:  
2                   a host security circuit, said host security circuit comprising:  
3                             at least one locally stored secret,  
4                             seed data;  
5                   a host processor for performing a non-reversible device authentication  
6     algorithm; and  
7                   means for reading data from a subsystem device;  
8                   a roaming security device as part of said subsystem device, said roaming security  
9     device comprising;  
10                  a subsystem processor for performing non-reversible computations;

11                   a memory component, connected to said subsystem processor, said  
12 memory circuit comprising at least one secret;  
13                   a communication circuit, connected to said subsystem processor, for  
14 communicating with said host security circuit;  
15                   said subsystem device being removably attached to said host system  
16 device, said host system being substantially inoperable without being attached to said subsystem  
17 device.

1           36.   (new) The host system device and subsystem device combination of claim 35,  
2 wherein said host security circuit sends a challenge to said roaming security device and said  
3 roaming security device provides a first response to said challenge, using said at least one secret,  
4 to said host security circuit.

1           37.   (new) The host security system device and subsystem device combination of  
2 claim 36, wherein said host security circuit reads said first response from said roaming security  
3 device and said host security circuit compares said first response with a first result of said non-  
4 reversible device authentication algorithm to determine if said first response and said first result  
5 match.

1           38.   (new) The host security system device and subsystem device combination of  
2 claim 35, wherein said roaming security device authenticates said host security circuit at  
3 substantially the same time as the host security circuit authenticates said roaming security  
4 device.

1           39.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein said host security system is a printer.

1           40.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein said subsystem device is a printer cartridge.

1           42.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein said host security circuit periodically checks the authenticity of said roaming  
3 security device.

1           43.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein communication data is encrypted prior to communication between said host  
3 system device and said subsystem device.

1           44.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein an attempt to physically access the circuitry of the roaming security device  
3 results in the destruction of data stored in said roaming security device.

1           45.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein said subsystem device further comprises a battery for at least partially  
3 powering said roaming security device.

1           46.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein said at least one locally stored secret is never communicated to said subsystem  
3 device.

1           47.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein said at least one secret is never communicated to said host device.

1           48.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein said non-reversible device authentication algorithm is a SHA-1 algorithm.

1           49.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein said host security circuit communicates with said subsystem device to  
3 authenticate said subsystem device and to determine at least one of whether said subsystem  
4 device is the proper type, brand, or age.

1           50.    (new) The host security system device and subsystem device combination of  
2 claim 49, wherein said host system is disabled if said subsystem device cannot be authenticated.

1           52.    (new) The host security system device and subsystem device combination of  
2 claim 35, wherein said subsystem device is a consumable device.

1           51.    (new) A subsystem device comprising:  
2                   a replaceable subsystem that operationally completes a host system;  
3                   a security device being a part of said replaceable subsystem, said security device  
4 comprising:  
5                   a first memory portion configured to store a device ID;  
6                   a second memory portion configured to store at least one device secret;

7                   a processor connected to said first and second memory portions, the  
8   processor configured to read the stored device ID from the first memory portion, the at least one  
9   stored device secret from the second memory portion and to perform a nonreversible  
10   computation using the device ID, the at least one device secret and a challenge as seeds; and  
11                   a communication circuit connected to the processor, said communication  
12   circuit configured to receive the challenge from a host device and to communicate a result of the  
13   nonreversible computation, performed by the processor, back to the host for authentication of  
14   said replaceable subsystem.

1           52.   (new) The subsystem device of claim 51, wherein said host device is disabled  
2   until a replaceable subsystem is installed and authenticated.

1           53.   (new) The subsystem device of claim 51, wherein said host is a printer device.

1           54.   (new) The subsystem device of claim 51, wherein said subsystem is a  
2   consumable device.

1           55.   (new) The subsystem of claim 51, wherein said subsystem is a printer cartridge.

1           56.   (new) The subsystem of claim 51, wherein said nonreversible computation is a  
2   SHA-1 computation.

1           57.   (new) The subsystem of claim 51, wherein said subsystem authenticates said  
2   host.

- 1           58.     (new) The subsystem of claim 51, wherein an attempt to physically access said
- 2     security device will result in the destruction of said device ID and said at least one device secret.